(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10066157 A**

(43) Date of publication of application: **06 . 03 . 98**

(51) Int. Cl **H04Q 7/38**
H04L 9/08
H04L 9/18
H04L 12/56

(21) Application number: **09149370**

(22) Date of filing: **06 . 06 . 97**

(30) Priority: **06 . 06 . 96 FI 96 962352**

(71) Applicant: **NOKIA MOBILE PHONES LTD**

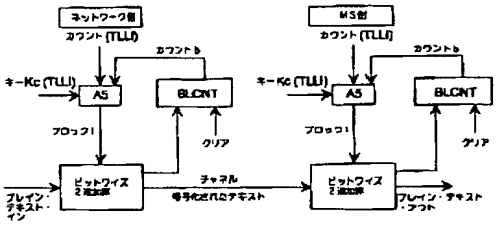
(72) Inventor: **KARPPANEN ARTO**
KARI HANNU
HAEMAELAEINEN JARI
JUOPPERI JARI

(54) **INFORMATION-CIPHERING METHOD AND DATA COMMUNICATION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To transfer data by mode of not ciphering a header field in a physical layer by dividing into function layers in which data transferring systems are different at each layer of different data frame structure.

SOLUTION: A not ciphered sub-block (plain text in) is ciphered from a network side and transferred to a mobile station(MS) side as a ciphered block (ciphered text). A block counter (BLCNT) is set to be an initial value by a set line signal (clear) at the time of starting a data frame of each adaptive layer and generates a data count (count (b)). A ciphering algorithm A8 calculates an output bit string (block 1) for each block from a prescribed ciphering key Kc and the count (b). A network side obtains a text by bit-adding a block 1 to the plain text.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－66157

(43)公開日　平成10年(1998)３月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｒ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｃ
	9/18					６５１
	12/56		9744－5K		11/20	１０２Ｚ

審査請求　未請求　請求項の数20　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－149370

(22)出願日　平成９年(1997)６月６日

(31)優先権主張番号　９６２３５２

(32)優先日　1996年６月６日

(33)優先権主張国　フィンランド（ＦＩ）

(71)出願人　590005612
ノキア　モービル　フォーンズ　リミティド
フィンランド国，エフアイエヌ－02150　エスポー，ケイララーデンティエ　４

(72)発明者　アルト　カルバネン
フィンランド国，エフイーエン－00210　ヘルシンキ，ペチュニエメンカトゥ　４　デー　64

(72)発明者　ハンヌ　カリ
フィンランド国，エフイーエン－02880　ベイッコラ，クラボンクヤ　９　ベー　９

(74)代理人　弁理士　石田　敬　（外３名）

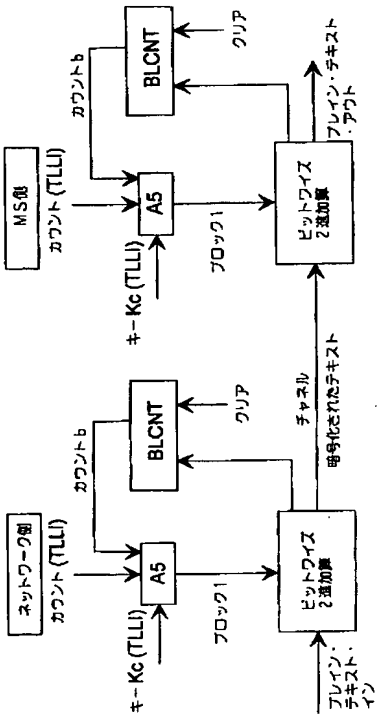
最終頁に続く

(54)【発明の名称】　情報の暗号化方法およびデータ通信システム

(57)【要約】

【課題】　転送されたデータがデータ・フレーム・モードにありかつデータ転送システムがデータ・フレーム構造が異なる層において異なることができるような機能層に分割されているデータ転送システムにおけるデータ転送の暗号化方法及び装置を提供する。

【解決手段】　一つ以上のデータ・フレームがアプリケーションによる情報から形成された一つ以上のデータ・パケットから生成されるデータ通信システムのデータ転送機器（ＭＳ，ＳＧＳＮ）間で転送された情報の暗号化方法が提供される。データ・フレームは、少なくともヘッダ・フィールド及びデータ・フィールドを含む。データ・パケットの少なくともある部分は、暗号化キー（Ｋｃ）を用いて暗号化される。データ・フレームに対して、同期データ（ＣＯＵＮＴ）が配属され、その値は、少なくとも各データ・フレームの伝送時に変えられる。



1

【特許請求の範囲】

【請求項１】　アプリケーションによって情報から形成された一つ以上のデータ・パケットから一つ以上のデータ・フレームが生成され、かつこれらのデータ・フレームは、少なくともヘッダ・フィールド及びデータ・フィールドを含む、データ通信システムのデータ転送機器（ＭＳ，ＳＧＳＮ）間で転送された情報の暗号化方法において、前記データ・パケットの少なくとも一つの部分は、暗号化キー（Ｋｃ）を用いて暗号化されかつ同期データ（ＣＯＵＮＴ）は、データ・フレームに配属されかつその値は、少なくとも各データ・フレームの伝送時に変えられることを特徴とする情報の暗号化方法。

【請求項２】　データ転送接続は、前記データ通信システムに接続された二つ以上のデータ転送機器（ＭＳ，ＳＧＳＮ）間で形成される前記方法において、個別の暗号化キー（Ｋｃ）が各接続に割り当てられ、同じデータ転送チャネルで、少なくとも二つの個別接続のデータ・フレームは、互いに独立に暗号化モードで転送することができることを特徴とする請求項１に記載の方法。

【請求項３】　前記データ・フレームは、少なくとも一つのサブ－ブロックに分割される前記方法において、前記同期データは、各接続に個別に割り当てられかつ初期値が接続の開始で設定されかつその値が各サブ－ブロックの伝送時に変えられるブロック・カウンタ（ＢＬＣＮＴ）を含むことを特徴とする請求項１または２に記載の方法。

【請求項４】　前記データ・フレームは、適応層（ＬＬＣ）で形成されることを特徴とする請求項１，２または３に記載の方法。

【請求項５】　前記適応層の前記データ・フレームは、リンク層（ＭＡＣ，ＲＬＣ，ＬＬＣ，Ｌ２）に転送され、前記リンク層のデータ・フレームは、伝送経路（Ｕｍ，Ｇｂ）への伝送のための前記適応層の前記データ・フレームから形成されることを特徴とする請求項４に記載の方法。

【請求項６】　前記同期データ（ＣＯＵＮＴ）は、次の少なくとも一つ：

－　前記リンク層のデータ・フレーム番号（ＬＬＣ＃）、

－　前記適応層のデータ・フレーム番号（ＳＤＵ＃）、

－　ルーティング・エリアの識別子（ルーティング・エリア＃）、

－　パケット・スイッチング・コントローラのエリアの識別子（ＳＧＳＮ＃）、

－　セルの識別子（Ｃｅｌｌ＃）

を含むことを特徴とする請求項５に記載の方法。

【請求項７】　前記データ・フレーム番号（ＳＤＵ＃）は、データ転送接続に結合されたデータ転送機器（ＭＳ，ＳＧＳＮ）において形成されかつ局所的に維持され、シーケンス番号は、接続の開始でその初期値に設定

2

されかつそれは、接続の間中に予め定義された方法で更新されることを特徴とする請求項６に記載の方法。

【請求項８】　前記リンク層のデータ・フレーム番号（ＬＬＣ＃）は、前記データ転送接続の一つのデータ転送機器（ＭＳ，ＳＧＳＮ）に維持されかつそれは、前記リンク層の前記データ・フレームにおける他のデータ転送機器に送付されることを特徴とする請求項６に記載の方法。

【請求項９】　前記データ転送接続は、ＧＰＲＳシステムのような、パケット・スイッチング・システムのデータ転送接続であることを特徴とする請求項１から８のいずれか一項に記載の方法。

【請求項１０】　前記データ転送接続は、ポイントーツウーポイント接続（ＰＴＰ）であることを特徴とする請求項１から９のいずれか一項に記載の方法。

【請求項１１】　前記データ転送接続は、ポイントーツウーマルチポイントーマルチキャスト（ＰＴＭ－Ｍ）またはポイントーツウーマルチポイントーグループ（ＰＴＭ－Ｇ）のような、マルチポイント接続であることを特徴とする請求項１から９のいずれか一項に記載の方法。

【請求項１２】　情報は、データ・サービス・プロバイダの前記データ転送機器（ＳＧＳＮ）とデータ・サービス・ユーザの前記データ転送機器（ＭＳ）の間で転送され、各接続に個別に割り当てられた暗号化キー（Ｋｃ）は、前記データ転送機器のキーパッドまたはスマート・カード（ＳＩＭ）を用いて、前記データ転送システムの暗号化モードで暗号化キー（Ｋｃ）を転送することによって前記データ転送機器（ＭＳ，ＳＧＳＮ）に設定されることを特徴とする請求項１１に記載の方法。

【請求項１３】　－　前記データ・サービス・プロバイダの前記データ転送機器（ＳＧＳＮ）から前記データ・サービス・ユーザの前記データ転送機器（ＭＳ）へ伝送されたデータだけが少なくとも部分的に暗号化され、

－　前記データ・サービス・ユーザの前記データ転送機器（ＭＳ）から前記データ・サービス・プロバイダの前記データ転送機器（ＳＧＳＮ）に伝送されたデータだけが少なくとも部分的に暗号化され、または、

－　両方の方向に伝送されたデータが少なくともある程度暗号化されることを特徴とする請求項１１または１２に記載の方法。

【請求項１４】　暗号化の開始で、データ転送が暗号化される方向を考慮しているデータは、データ転送機器へ伝送されることを特徴とする請求項１３に記載の方法。

【請求項１５】　前記適応層の前記データ・フレームのある部分だけが暗号化され、各データ・フレームの暗号化のデータは、該データ・フレームの前記ヘッダ・フィールドで伝送されるのが最も好ましいことを特徴とする請求項１から１４のいずれか一項に記載の方法。

【請求項１６】　データ通信システムのデータ転送機器（ＭＳ，ＳＧＳＮ）間で転送された情報の暗号化手段、

前記情報の一つ以上のデータ・パケットを形成する手段、及び前記データ・パケットのデータ・フレームを形成する手段を備えているデータ通信システムにおいて、前記情報の暗号化手段は、

－　暗号化キー（Ｋｃ）によりデータ・パケットを暗号化する手段、

－　データ・フレームに同期データ（ＣＯＵＮＴ）を配属する手段、

－　各データ・フレームの前記伝送で前記同期データ（ＣＯＵＮＴ）の前記値を変える手段、及び

－　レシーバ側の前記データ転送機器において同期データを解釈する手段を少なくとも備えていることを特徴とするデータ通信システム。

【請求項１７】　前記データ転送手段は、少なくとも一つの移動局（ＭＳ）を備えていることを特徴とする請求項１６に記載のデータ通信システム。

【請求項１８】　前記データ転送手段は、少なくとも一つの基地局（ＢＴＳ）を備えていることを特徴とする請求項１６に記載のデータ通信システム。

【請求項１９】　前記移動局（ＭＳ）は、ＧＳＭ移動局であることを特徴とする請求項１７に記載のデータ通信システム。

【請求項２０】　前記基地局（ＢＴＳ）は、ＧＳＭ基地局であることを特徴とする請求項１８に記載のデータ通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、少なくともヘッダ・フィールド及びデータ・フィールドを備えている一つ以上のデータ・フレームがアプリケーションにより情報から形成された一つ以上のデータ・パケットから形成されるデータ通信システムにおけるデータ通信機器間で転送される情報の暗号化方法に関する。更に本発明は、データ転送機器間で転送される情報の暗号化手段、情報から一つ以上のデータ・パケットを形成する手段及びデータ・パケットからデータ・フレームを形成する手段を備えているデータ通信システムに関する。

【０００２】

【従来の技術】別個のデータ転送機器間のデータ転送は、それらの間でそのときのデータが転送されるべきそれらのデータ転送機器がデータ転送に必要な時間の間互いに結合されるような方法で達成することができる。この場合、その結合は、ユーザがデータ転送を停止するまで維持される。そのような場合には、結合時間のほとんどの部分は、ユーザによって供給されるコマンドを入力することに費やされかつ時間のほんの少しの部分が実際のデータ転送である。これは、例えば、同時ユーザの最大数を制限する。別の可能性は、いわゆるパケット切替えデータ伝送を利用することである。この場合には、データは、パケット・モードにおいてデータ転送機器間で

転送され、そのような場合には、パケット間の時間は、自由に利用可能でありかつ他のデータ転送機器によって用いることができる。この場合には、同じセルラー・エリアにある移動局が同じ転送チャネルを用いることができるので、同時のユーザの数は、特にセルラー・ネットワークのような、無線データ転送ネットワークにおいて、増大することができる。一つのそのようなセルラー・システムは、パケット・モードデータ転送サービスＧＰＲＳ（ジェネラル・パケット・ラジオ・サービス）が開発されたＧＳＭ（グループ・スペシャル・モービル）システムである。図１は、ＧＰＲＳシステムの動作における主要ブロックのブロック図を示す。パケット・スイッチング・コントローラＳＧＳＮ（サービングＧＰＲＳサポート・ノード）は、セルラー・ネットワーク側のパケット・スイッチング・サービスの動作を制御する。パケット・スイッチング・コントローラＳＧＳＮは、移動局ＭＳのサインーオン及びサインーオフ、移動局ＭＳの位置の更新及びそれらの正しい宛先へのデータ・パケットのルーティングを制御する。移動局ＭＳは、無線インターフェイスＵｍを通して基地局サブシステムＢＳＳに接続される（図１）。基地局サブシステムは、ＢＳＳ－ＳＧＳＮインターフェイスＧｂを通してパケット・スイッチング・コントローラＳＧＳＮに接続される。基地局サブシステムＢＳＳでは、基地局ＢＴＳ及び基地局コントローラＢＳＣは、ＢＴＳ－ＢＳＣインターフェイスＡｂｉｓによって相互に接続されている。移動局ネットワークにおけるパケット・スイッチング・コントローラＳＧＳＮの位置は、例えば、どの技術的実現（インプリメンテーション）が用いられるかにより変えることができる。図１では、パケット・スイッチング・コントローラＳＧＳＮが基地局サブシステムＢＳＳの外側に示されているが、パケット・スイッチング・コントローラＳＧＳＮは、例えば、基地局サブシステムＢＳＳに接続される基地局ＢＴＳの一部または基地局コントローラＢＳＣの一部として設けることができる。

【０００３】ＧＰＲＳシステムは、例えば、本発明の出願日以前の日付を有する草案ＧＳＭ０１．６０、ＧＳＭ０２．６０、ＧＳＭ０３．６０及びＧＳＭ０４．６０に記載されている。移動局ＭＳ及びパケット・スイッチング・コントローラＳＧＳＮの両方の動作は、図２に示したように、それぞれが異なる機能を供給している種々の層に分割することができる。国際標準化機構、ＩＳＯは、データ転送を異なる機能層にグループ化するためのＯＳＩ（オープン・システム・インターコネクション）モデルを公式化した。このモデルでは、全てのデータ通信システムにおいて必ずしも必要ではない７つの層がある。

【０００４】移動局ＭＳとパケット・スイッチング・コントローラＳＧＳＮの間で、ユーザによって伝送されたデータ及び制御信号のような、転送可能情報は、データ

・フレーム・モードで交換されるのが好ましい。各層のデータ・フレームは、ヘッダ・フィールド及びデータ・フィールドからなる。図２は、また、異なる層のＧＰＲＳシステムに用いられているデータ・フレームの構造を示す。

【０００５】データ・フィールドに含まれた情報は、例えば、移動局のユーザによって入力されたデータまたは信号データでよい。データ・フィールドは、無線経路にそれを伝送する前にできるだけ確実に保護されなければならない機密情報を含みうる。そのような場合には、暗号化は、パケット・スイッチング・コントローラＳＧＳＮとそれに接続された移動局ＭＳとの間の全ての同時接続において、個別の暗号化キーが用いられるような方法で実行されなければならない。逆に言えば、移動局ＭＳは、共有無線経路資源を用いるので、即ち、多くの異なる接続における情報が同じチャネルで、例えば、異なる時間間隔で、転送されるので、データ・フィールドの暗号化に用いられたのと同じ暗号化キーによってデータ・フレームのアドレス・データを暗号化することは、好ましくない。この場合には、各移動局は、関係しているチャネルで伝送された全てのメッセージを受信しかつメッセージが向けられた移動局を識別するために少なくともアドレス・データの暗号化を暗号解読すべきである。また、パケット・スイッチング・コントローラＳＧＳＮは、どの暗号化キーを用いるべきか分からない。

【０００６】次に、ＧＰＲＳシステムの層の動作機能を示す。最下位層は、パケットを伝送しかつ受信するためのチャネルを割り当てることのような、移動局ＭＳと基地局サブシステムＢＳＳの間の通信における無線経路の使用を制御するＭＡＣ（メディア・アクセス・コントロール）層と呼ばれる。最下位レベルにおけるパケット・コントローラＳＧＳＮと基地局サブシステムの間のデータ伝送は、標準Ｑ．９２１によるＬＡＰＤプロトコル、フレーム・リレー・プロトコルまたは同等物のような、リンク層プロトコルが用いられる、Ｌ２層（リンク層）で実行される。Ｌ２層は、ＧＰＲＳ仕様による品質またはルーティング・データも更に含みうる。層Ｌ２は、ＯＳＩモデルの物理層及びリンク層の特性を有する。基地局サブシステムＢＳＳとパケット・コントローラＳＧＳＮの間の物理伝送回線は、例えば、パケット・コントローラＳＧＳＮがシステムにおいて配置された場所に依存する。

【０００７】ＭＡＣ層の上に、ＲＬＣ層（ラジオ・リンク・コントロール）があり、その機能は、無線経路へ伝送すべく固定された大きさのパケットにＬＬＣ層によって形成されたデータ・フレームを分割すること及び必要であればそれらの伝送及び再伝送である。ＧＲＰＳシステムにおけるパケットの長さは、１ＧＳＭタイム・スロットの長さ（おおよそ０．５７７ｍｓ）である。

【０００８】ＬＬＣ（ロジック・リンク・コントロール）層は、移動局ＭＳとパケット・コントローラＳＧＳＮの間に信頼できる伝送リンクを提供する。ＬＬＣ層は、例えば、誤り検査データを伝送されたメッセージに加え、それにより、それらの不正確に受信されたメッセージを訂正しようとし、必要なときには、メッセージは、再伝送することができる。

【０００９】ＳＮＤＣ層（サブーネットワーク・ディペンデント・コンバージェンス）は、伝送された情報のプロトコル変換、圧縮、セグメンテーション及び上部層からくるメッセージのセグメンテーションのような機能を備えている。更に、暗号化及び暗号解除は、ＳＮＤＣ層で達成される。ＳＮＤＣフレームの構造も図２に示されている。ＳＮＤＣフレームは、ＳＮＤＣヘッダ・フィールド（ＳＮＤＣヘッダ）及びＳＮＤＣデータ・フィールド（ＳＮＤＣデータ）を備えている。ＳＮＤＣヘッダ・フィールドは、プロトコル・データ（ネットワーク・レイヤー・サービス・アクセス・ポイント・アイデンティティ、ＮＬＳＩ）及び、圧縮、セグメンテーション及び暗号化の決定のような、ＳＮＤＣ制御データからなる。ＳＮＤＣ層は、上部レベルで用いられるプロトコルとＬＬＣ層（リンク層）のプロトコルの間のプロトコル・アダプタとして機能する。

【００１０】伝送された情報は、ＧＰＲＳシステムによるメッセージまたはインターネット・プロトコル（ＩＰ）のパケットのような、あるアプリケーションからＳＮＤＣ層へデータ・パケットとしてやってくるのが好ましい。アプリケーションは、例えば、移動局のデータ・アプリケーション、テレコピー・アプリケーション、移動局へのデータ伝送リンクを有するコンピュータ・プログラム、等であることができる。

【００１１】ＭＡＣ層、ＲＬＣ層、ＬＬＣ層及びＬ２層は、ＯＳＩモデルの層２で記述される特性を含む。上記した層及びＯＳＩモデルで記述された層は、しかしながら、明確な一貫性がない。ＳＮＤＣフレームは、ＬＬＣヘッダ・フィールドがフレームに加えられるＬＬＣ層へ転送される。ＬＬＣヘッダ・フィールドは、テンポラリ・ロジカル・リンク・アイデンティティ（ＴＬＬＩ）及びＬＬＣ制御部分からなる。パケット・コントローラＧＰＲＳは、移動局ＭＳとパケット・コントローラＧＰＲＳの間の各データ伝送リンクに対するＴＬＬＩ識別子（アイデンティティ）を確立する。このデータは、どのデータ伝送リンクに各メッセージが属するかを画定するためのデータ伝送で用いられる。同時に、同じＴＬＬＩ識別子は、一つのデータ伝送リンクにおいてのみ用いることができる。リンクの終了後、リンクで用いられたＴＬＬＩ識別子は、その後形成される新しいリンクへ割り当てられることができる。ＬＬＣ制御部分は、誤り無しデータの転送を確実にするためのフレーム番号及びコマンド型（インフォ(info)、肯定応答、再伝送要求、等）を規定する。

【００１２】ＧＳＭシステムにおける暗号化は、ビット毎の暗号化として物理層で実行される、即ち、無線経路へ伝送されたビット・ストリームは、暗号化キーＫｃを用いて、本質的に知られたアルゴリズムＡ５を用いて形成される伝送されたデータ暗号化ビットへ加えることによって形成される。アルゴリズムＡ５は、データ転送に割り当てられたチャネルの物理層で伝送されたデータ及び信号情報を暗号化する（トラフィック・チャネル、ＴＣＨまたはデディケーティド・コントロール・チャネル、ＤＣＣＨ）。

【００１３】伝送されたメッセージの同期は、アルゴリズム５が特別の同期データ（ＣＯＵＮＴ）により駆動されるような方法で確保される。同期データＣＯＵＮＴは、ＴＤＭＡフレーム番号に基づき形成される。次いで、アルゴリズムＡ５によって形成された各１１４－ビット・ブロックの内容は、フレーム番号及び暗号化キーＫｃにのみ依存する。

【００１４】暗号化キーＫｃの設定は、割り当てられたチャネルの通信トラフィックがまだ暗号化されておらずかつ用いられている移動局ネットワークが移動局ＭＳを識別したときの段階で実行されるのが最も好ましい。ＧＳＭシステムにおける識別では、移動局を識別しかつ移動局に記憶されている、インターナショナル・モービル・サブスクライバー・アイデンティティ、ＩＭＳＩが用いられるか、または、加入者識別子に基づき形成されている、テンポラリ・モービル・サブスクライバ・アイデンティティ、ＴＭＳＩが用いられる。移動局では、また、加入者識別キー、Ｋｉが記憶されている。加入者識別キーＫｉは、また、移動局ネットワークによっても知られている。

【００１５】暗号化キーＫｃが移動局ＭＳ及び移動局ネットワークによってのみ知られるということを確実にするために、基地局サブシステムＢＳＳから移動局ＭＳへの暗号化キーの伝送は、間接的である。次いで、基地局サブシステムＢＳＳでは、移動局ＭＳへ伝送されるランダム・アクセス・ナンバー、ＲＡＮＤが形成される。暗号化キーＫｃは、図３に示したような、アルゴリズムＡ８を用いて、ランダム・アクセス・ナンバーＲＡＮＤから及び加入者識別キーＫｉから形成される。暗号化キーＫｃの計算及び記憶は、移動局ＭＳ及び移動局ネットワークの両方で実行される。

【００１６】移動局ＭＳと基地局サブシステムＢＳＳの間のデータ転送は、接続の開始では暗号化されない。暗号化されたモードへの遷移は、基地局サブシステムＢＳＳが、ここでは“スタート・サイファー(start cipher)”と呼ばれるある一定のコマンド（暗号化されていない）を移動局へ伝送するような方法で進められるのが好ましい。移動局ＭＳがコマンド“スタート・サイファー”を受信した後、それは、伝送されたメッセージの暗号化及び受信したメッセージの暗号解読を開始する。それに対応して、基地局サブシステムＢＳＳは、基地局サブシステムが移動局によって伝送された暗号化されたメッセージを受信しかつ正しく暗号を暗号解読した後に、移動局へ伝送されるメッセージの暗号化を開始する。

【００１７】

【発明が解決しようとする課題】上述した暗号化では、同期は、例えば、物理層のＴＤＭＡフレーム番号に基づいていた。全てのアプリケーションにおいて、特に、パケット切替えデータ伝送方法におけるような、異なる接続（コネクション(connection)）に属する情報が同じチャネルで伝送されるときに、それを用いることができない。

【００１８】欧州特許ＥＰ－０６８９３１６号公報では、例えば、暗号化キーを備えている暗号化データが伝送されたデータ・フレームに配属（アタッチ(attatch)）されるような、データ転送の暗号化に対する方法が示されている。米国特許ＵＳ－５，３１９，７１２号公報は、リンク層のデータ・フレームにシーケンス番号が配属されかつデータ・フレームが暗号化されるようなデータ転送の暗号化に対する方法及び装置を備えている。従来技術によるこれらの暗号化方法の欠点は、例えば、受信者が、暗号解読することなしでは、受信したデータ・フレームが誰に向けられたものかが分からず、不必要なデータ・フレームの受信及び暗号解読がシステムの効率における低下をもたらす。

【００１９】本発明の目的は、転送されたデータがデータ・フレーム・モードにありかつデータ転送システムがデータ・フレーム構造が異なる層において異なることができるような機能層に分割されているデータ転送システムにおけるデータ転送の暗号化方法及び装置を提供することである。

【００２０】

【課題を解決するための手段】本発明による方法は、データ・パケットの少なくともある部分が暗号化キーによって暗号化され、かつ同期データがデータ・フレームに配属され、かつその値が少なくとも各データ・フレームの伝送で変更されることを特徴とする。本発明によるシステムは、情報を暗号化する手段が少なくとも

－　データ・パケットを暗号化キーで暗号化する手段、

－　同期データをデータ・フレームに配属する手段、

－　各データ・フレームの伝送で同期データの値を変更する手段、及び

－　受信者のデータ転送機器における同期データを解釈する手段を備えていることを特徴とする。

【００２１】従来技術による暗号化方法と比較して、相当な利点が本発明によって達成される。本発明による方法では、物理層のデータ・フレームのヘッダ・フィールドは、暗号化されていないモードで伝送することができるか、または現在知られている方法を暗号化に用いることができる。本発明の好ましい実施例による方法では、

暗号化キーは、物理層の各伝送ブロックに対して変更され、暗号化キーについての知識なしで暗号解読することは、実質的に不可能である。本発明による方法を用いることによって、部分的暗号化を実現することが更に可能であり、伝送されたデータ・フレームの一部だけが暗号化される。この場合には、例えば、広告が暗号化されないままに送付されかつ暗号化されたデータ・フレームを受信しかつそれらを暗号解読する権利を有するものに対してだけ他の情報が暗号化されて送付されることができる。

【００２２】

【発明の実施の形態】本発明は、添付した図面を参照して以下により詳細に説明される。以下において、本発明は、ＧＳＭシステムで実現されたパケット切替えサービスＧＰＲＳにより具体化されているが、しかしながら、本発明は、このシステムだけに限定されるものではない。

【００２３】本発明では、例えば、ＧＰＲＳシステムにおける、データ・フレームの伝送にそれが適用できるように調整されるＧＳＭシステムの暗号化のような、できるだけ多くの既存の暗号化技術が利用されるインプリメンテーションを目的にしている。本発明の一つの利点は、ポイント間接続（ＰＴＰ（ポイントーツウーポイント）接続）、多重ポイント接続｛（ＰＴＭ－Ｍ（ポイントーツウーマルチポイントーマルチキャスト）；ＰＴＭ－Ｇ（ポイントーツウーマルチポイントーグループ）｝、その他、等のような、多くの動作モードにそれを適用することができるということである。暗号化方法は、ＴＬＬＩ識別子に基づき主に分類される。明確なＴＬＬＩ識別子は、移動局ＭＳとパケット・スイッチング・コントローラＳＧＳＮの間の各接続型に対して割り当てられる。以下の異なる型は、本標準によるＧＰＲＳシステムにおける使用に対して利用可能である：

－　ポイントーツウーポイント（ＰＴＰ）は、移動局ＭＳとパケット・スイッチング・コントローラＳＧＳＮの間の通信に独自のＴＬＬＩ識別子を用いる。

【００２４】－　ポイントーツウーマルチポイントーマルチキャスト（ＰＴＭ－Ｍ）は、移動局ＭＳとマルチキャスト・サービス・プロバイダの間の通信に対して割り当てられたＴＬＬＩを用いる。

－　ポイントーツウーマルチポイントーグループ（ＰＴＭ－Ｇ）は、移動局グループ内の移動局ＭＳのマルチキャスト・サービス・プロバイダを介して相互通信に対して割り当てられたＴＬＬＩを用いる。

【００２５】ポイントーツウーポイント接続は、リンク層レベルで肯定応答モードを一般に用いる、即ち、伝送のレシーバ（受信器）は、正しい受信の肯定応答としてデータを伝送する。ポイントーツウーマルチポイント接続では、データ・フレームは、肯定応答が伝送されない動作モードを用いて通常伝送される。この説明において

既に先に示したように、異なる接続（コネクション(connection)）のデータが同じチャネルで伝送されるシステムでは、各接続に対して独自の暗号化キーによってデータ・フレームのヘッダ・フィールドを暗号化するのは好ましくない。この場合には、データ・フレームは、物理層以外の他の層で少なくとも部分的に暗号化される。ＧＰＲＳシステムでは、暗号化は、ＬＬＣ層で実行される。伝送されたデータは、データ・フレームの各ビットに対して、暗号化ビット・ストリングの対応ビットが合計されるような方法で暗号化される。暗号化ビット・ストリングは、個別かつ独自の暗号化キーＫｃを用いて暗号化アルゴリズムによって形成されているのが好ましい。暗号化アルゴリズムは、例えば、ＧＳＭシステムから知られたＡ５アルゴリズムである。

【００２６】正しいアドレスに加えて、データ・フレームがレシーバ（受信器）でシーケンス化することができることを確実にしなければならない。これは、既に知られた方法で実現することができ、同期データＣＯＵＮＴ（カウント）は、暗号化アルゴリズムに入力され、レシーバが、暗号解読後に、データ・フレームのシーケンスを見出すことができる。例えば、ＴＤＭＡ（タイム・ディビジョン・マルチプル・アクセス(Time Division Multiple Access)）システムでは、ＧＳＭのように、物理層のデータ・フレームに番号を付けるためにＴＤＭＡフレーム番号を用いることができる。しかしながら、ＧＰＲＳシステムのパケット・スイッチング・コントローラＳＧＳＮは、ＴＤＭＡフレーム番号を知らず、そこでこの発明ではデータ・フレームを同期するための方法が開発され、この方法でデータ・フレームのシーケンス番号（データ・フレーム番号）が同期データとして用いられる。それゆえに、各伝送されたブロックの内容は、例えば、フレーム番号及び暗号化キーＫｃによって決定される。

【００２７】暗号化されるべきデータの量は、異なる接続において変わるが、暗号化が伝送されたデータを好ましくは標準長さのサブーブロックに分割することによって実行できるので、これは、本発明のアプリケーションにおいて重要ではない。次いで、各サブーブロックの第１のビットが暗号化アルゴリズムの第１のビットによって、サブーブロックの第２のビットが暗号化アルゴリズムの第２のビットによって等、暗号化される。ＧＰＲＳシステムでは、サブーブロックの長さは、例えば、本ＧＳＭシステムにおけるような、１１４ビットでありうる。好ましくは、サブーブロックの長さは、また、バイトの長さにより分割可能でもありうる。多くのアプリケーションでは、バイトの長さは、８であり、サブーブロックに対する適切な長さは、６４ビットでありうる。

【００２８】ＧＳＭシステムでは、移動局ＭＳは、一度に一つの暗号化キーＫｃだけを用いることができる。ＧＰＲＳシステムでは、移動局は、各接続が異なる手段に

よって形成されているのが好ましい個別の暗号化キーＫｃを有しているのが最も好ましい多くの異なる型のアクティブ接続（ＰＴＰ，ＰＴＭ）を同時に有することができるので、移動局ＭＳ毎に一つの暗号化キーは、全ての情況において必ずしも十分ではない。それゆえに、暗号化されたデータ・フレームは、用いられた暗号化キーＫｃ、同期データＣＯＵＮＴ及び可能であればまたＴＬＬＩに配属されたブロック・カウンタＢＬＣＮＴの値ＣＯＵＮＴｂ（カウントｂ）を含む。図４は、暗号化されていないサブーブロック（プレイン・テキスト・イン）がネットワークから移動局へ暗号化されて（暗号化されたテキスト）転送される情況における略ブロック図として本発明による好ましい暗号化方法を示す。この実施例では、また、ブロック・カウンタの値ＣＯＵＮＴｂは、暗号化ブロックＢＬＯＣＫ１の決定において用いられる。ブロック・カウンタは、好ましくは各適応層のデータ・フレームの開始において、設定ライン“クリア(clear)”によりその初期値に設定することができる。ネットワーク側及び移動局ＭＳの両方において、同期データＣＯＵＮＴの値は、暗号化アルゴリズムＡ５に入力された同期データＣＯＵＮＴの値及び暗号化キーＫｃで、各伝送されたブロックについて計算される。伝送側では、出力ビット・ストリング（ＢＬＯＣＫ１（ブロック１））は、サブーブロック（プレイン・テキスト・イン）に加算される。暗号化されたサブーブロックは、移動局ＭＳへチャネル内を転送される。移動局ＭＳは、受信した暗号化サブーブロックと暗号化アルゴリズムＡ５の出力ビット・ストリング（ＢＬＯＣＫ１）とを加算することによってそれ相応にそれを暗号解読し、加算結果として、伝送されたサブーブロックに対応している未だ暗号化していないサブーブロック（プレイン・テキスト・アウト）が得られる。図５は、略ブロック図として本発明による別の好ましい暗号化方法を示す。この実施例は、主にブロック・カウンタＢＬＣＮＴが用いられていないということにおいて図４の実施例とは異なる。

【００２９】フレーム・シーケンス番号の一般的な長さは、６から８ビットである。暗号化機密の観点から、ＣＯＵＮＴ変数としてのこの値だけでは十分でなく、従って、また、フレーム・シーケンス番号、例えば、基地局識別子に加えて他の変数を同期データのＣＯＵＮＴ値の決定に用いることができる。使用中の移動局が基地局の変更についてパケット・スイッチング・コントローラＳＧＳＮに知らせるので、基地局識別子は、ネットワーク及び移動局の両方によって知られている。それゆえに、基地局の変更によりこの実施例における同期データのＣＯＵＮＴ値が変わる。

【００３０】ポイントーツウーポイント接続モードでは、次の値は、同期データのＣＯＵＮＴ値の決定において利用可能である：

ａ）適応層（ＳＮＤＣ）に運ばれるロジカル・リンク・コントロール(LogicalLink Control)層のフレーム番号（ＬＬＣフレーム番号、ＬＬＣ＃）。

ｂ）それが接続の両端で維持されるときに接続の開始で初期化されるかまたは伝送されたデータ・フレームに配属されることができる適応層のデータ・フレーム番号（ＳＮＤＣデータ・ブロック番号、ＳＤＮ＃　）。

【００３１】ｃ）識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるルーティング・エリアの識別子（ルーティング・エリア＃）。

ｄ）識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるパケット・スイッチング・コントローラのエリアの識別子（ＳＧＳＮ＃）。

【００３２】ｅ）識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られる基地局の識別子（Ｃｅｌｌ＃）。ポイントーツウーマルチポイント接続モードでは、次の値は、同期データのＣＯＵＮＴ値の決定において利用可能である：

ａ）ＳＮＤＣデータ・フレーム内に伝送される適応層のデータ・フレーム番号（ＳＮＤＣデータ・ブロック番号、ＳＤＵ＃）

ｂ）識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるルーティング・エリアの識別子（ルーティング・エリア＃）。

【００３３】ｃ）識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるパケット・スイッチング・コントローラのエリアの識別子（ＳＧＳＮ＃）。

ｄ）識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られる基地局の識別子（Ｃｅｌｌ＃）。

【００３４】更に、両方の接続モードにおいて、同じ暗号化ビット・ストリングがシーケンシャル・データ・フィールドの暗号化で用いられないので、ブロック・カウンタＢＬＣＮＴの値を用いることができ、侵入者にとって、暗号化されたデータ・フィールドのクラッキングをさらに困難にする。さもなければ、再計算が適応層のデータ・フレームの各伝送に対して一度だけ実行される。適応層のデータ・フレームの長さは、数千ビットでありうるし、暗号化アルゴリズムが十分に何度も計算されないならば暗号化キーを見出すことが可能でありうる。

【００３５】同期データＣＯＵＮＴを定義している上記変数は、単独または組合せのいずれかで用いることができる。それゆえに変数のあるものは、データ・フレーム内のレシーバへ送付されなければならないしかつそれらのあるものは、局所的に管理することができる。局所的に管理される変数の使用は、機密のレベルを増大しかつある程度までそれは、転送されたデータの量を低減する。次の表は、同期データＣＯＵＮＴのコンテンツの例

13　　14

を示す。表１．１は、本発明の最も好ましい実施例による同期データを示しかつその中に、ブロック・カウンタＢＬＣＮＴが用いられ、かつ表１．２は、本発明の別の好ましい実施例を示しかつその中に、基地局の識別子が＊ブロック・カウンタＣＯＵＮＴｂの値の代わりに用いられている。

【００３６】

【表１】

表１．１

ビット／モード	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
PTP	SDU #（ローカル又は配送した）								LLC #（配送した）						COUNTb							
PTM	SDU #（配送した）								1	1	1	1	1	1	COUNTb							

【００３７】

【表２】

表１．２

ビット／モード	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
PTP	SDU #（ローカル又は配送した）								LLC #（配送した）						セル#、ルーティング・エリア#、又はSGSN #（ローカル）							
PTM	SDU #（配送した）								1	1	1	1	1	1	セル#、ルーティング・エリア#、又はSGSN #（ローカル）							

【００３８】次に、暗号化キーＫｃの設定を説明する。暗号化キーＫｃの設定は、ネットワーク・オペレータがそれを必要とする度にネットワークによって起動される。更に、独自の暗号化キーが各ＴＬＬＩ接続に対して生成されなければならない。暗号化キーＫｃ－ＴＬＬＩ識別子ペアの表は、パケット・スイッチング・コントローラＳＧＳＮ及び移動局ＭＳの両方に維持されるのが最も好ましい。暗号化キーの設定は、異なる接続型に対して異なる。

【００３９】ポイントーツウーポイント接続では、暗号化キーＫｃは、ランダム・アクセス番号ＲＡＮＤを用いて間接的に伝送される。暗号化キーＫｃは、ちょうどＧＳＭシステムにおけるように、アルゴリズムＡ８を用いて好ましくはランダム・アクセス番号ＲＡＮＤから及び移動局の加入者識別キーＫｉからＧＰＲＳシステムで形成される。移動局の識別キーは、移動局のＳＩＭ（サブスクライバ・アイデンティティ・モジュール(Subscriber Identity Module)）カード及びネットワークのオーセンティケーション・センターＡｕＣに記憶されている。

【００４０】マルチポイント接続では、同じサービスに接続される全ての移動局は、同じ暗号化キーＫｃを用いる。暗号化キーＫｃは、サービスへの接続が生成されるときに起動される。暗号化キーＫｃは、異なる方法を用いて移動局ＭＳに入力することができる。マルチポイント・サービス・プロバイダは、例えば、暗号化されたモードで、暗号化キーを入力することができ、移動局ＭＳは、マルチポイント接続へのアクセスを得る前にポイントーツウーポイント接続を通してパケット・スイッチング・コントローラＳＧＳＮにログされなければならない。ポイントーツウーポイント接続のログオン段階中に、暗号化キーＫｃは、接続に対して定義されかつ、それは、それが移動局ＭＳへ伝送されるときにマルチポイント接続の暗号化キーの暗号化に用いられる。

【００４１】マルチポイント接続の暗号化キーは、また、例えば、ＰＩＮコード、のような、移動局ＭＳのキーパッドを用いて、入力することができるか、または一種のＳＩＭカードは、他のパラメータの中で、暗号化キーＫｃが記憶されているところで用いることができる。暗号化キーＫｃは、暗号化キーを先のパケット・スイッチング・コントローラから新しいものへ送付することができるので、移動局ＭＳが別のパケット・スイッチング・コントローラＧＰＲＳのエリアへその位置を変えるときに再生成される必要がない。

【００４２】クリア・テキスト・モードから暗号化モードへの遷移は、パケット・スイッチング・コントローラＧＰＲＳが特別な“スタート・サイファー(start cipher)”コマンドをクリア・テキストで伝送するような方法で進行するのが好ましい。移動局ＭＳでは、移動局によって“スタート・サイファー”コマンドが正しく受信された後に伝送の暗号化及び受信の暗号解読が開始する。パケット・スイッチング・コントローラＧＰＲＳ側では、暗号化は、パケット・スイッチング・コントローラが移動局ＭＳによって伝送されたメッセージを受信しかつそれを暗号解読した後にそれ相応に開始する。上記動作は、その主な部分において、ＧＳＭシステムの暗号化の開始に対応する。

【００４３】あるパケット・スイッチング・アプリケーションでは、暗号化は、また、一方向へ行くメッセー

ジ、即ち、移動局ＭＳからパケット・スイッチング・コントローラＧＰＲＳへのまたはパケット・スイッチング・コントローラＧＰＲＳから移動局ＭＳへのメッセージだけが暗号化されるような方法で適用することができる。このようなアプリケーションは、例えば、通常は、暗号されないで伝送される広告の送付を含む。

【００４４】更に、本発明による暗号化は、適応層ＳＮＤＣの伝送されたデータ・フレームのある部分だけが暗号化されるような方法で適用することもできる。この場合には、一つの暗号化ビットが適応層のデータ・フレームに加えられるのが最も好ましくかつそれは、考慮するデータ・フレームが暗号化されるかまたは暗号化されていないかを示す。例えば、暗号化ビットが値ゼロを有するとき、データ・フレームは、暗号化されておらず、暗号化ビットが値１を有するとき、データ・フレームは、暗号化されている。これは、例えば、サービスへのアクセス権利が登録または同等物を必要とするような情況において、用いることができ、登録されたユーザは、暗号化されたデータ・フレームを暗号解読することができる。他のユーザに対して、サービス・プロバイダは、暗号化されていないデータ・フレームのサービス及び広告に関する情報を送付することができる。

【００４５】図６の（ａ）は、好ましい実施例によるリンク層のデータ・フレーム構造の例を示す。データ・フレームのヘッダ・フィールド（フレーム・ヘッダ）は、３バイトのＴＬＬＩ識別子及び２バイトの制御部分（コントロール(Control)）を含む。バイトは、既に知られているように、８つの２進情報（ビット）を含む。データ・フレームの情報フィールドは、伝送された情報を含む。情報フィールドの長さは、変わりうる。データ・フレームは、また、例えば、誤り訂正情報を含む２バイトの検査フィールド（チェック・シーケンス(Check sequence)）を含む。

【００４６】図６の（ｂ）は、データ・フレームが情報送付及びシステム・スーパーバイザリー・データ・フレーム（インフォメーション＋スーパーバイザリ(information+ supervisory)）であるときの図６の（ａ）のデータ・フレームの制御部分の構造を示し、その中で、Ｃ／Ｒは、それがコマンドまたは応答の質問（コマンド／レスポンス(Command/Response)であるかどうかを示す、Ｓ１及びＳ２は、スーパーバイザリ・コマンドの型を記述し、Ｎ（Ｓ）は、送信順序の番号（送信順序番号(Send sequence number)）であり、Ｐ／Ｆは、それが確認要求メッセージ（Ｐ）または確認メッセージ（Ｆ）の質問であるであるかを示し、（ポル／ファイナル(Poll/Final)）、そしてＮ（Ｒ）は、受信順序の番号（受信順序番号(Receive sequence number)）である。

【００４７】図６の（ｃ）は、データ・フレームがシステム・スーパーバイザリ・データ・フレーム（スーパーバイザリ(Supervisory)）であるときの図６の（ａ）のデータ・フレームの制御部分の構造を示す。ビットの意味は、上述した。図６の（ｄ）は、データ・フレームが番号なしデータ・フレーム（アンナンバード(Unnumbered)）のときの図６の（ａ）のデータ・フレームの制御部分の構造を示し、その中で、Ｍ１－５は、番号なしコマンド及び応答であり、Ｇ／Ｄは、それが制御またはデータ・フレームの質問であることを示し（コントロール／データ(Control/Data)）、そしてｘ－ビットは、重要でない。

【００４８】図７は、好ましい実施例による適応層のポイントーツウーポイント接続を有するデータ・フレーム構造の例を示す。第１のバイトは制御データを含み、その中で、

－　Ｍは、それがアプリケーションによって形成された情報の最後のセグメントの質問であるかどうかを示し、
－　Ｅは、暗号化が使用中であるかどうかを示し、
－　Ｐｒｉは、優先分類(priority classification)を示し、
－　ＮＬＳＩは、例えば、
－ＴＣＰ／ＩＰ、
－ＣＬＮＰ、
－Ｘ．２５、
－ＧＰＲＳ、等

であるような、プロトコル・データを示す。

【００４９】図８は、好ましい実施例による適応層のマルチポイント接続を有するデータ・フレーム構造の例を示す。ビットの意味は、上述した。本発明は、移動局ＭＳ、基地局サブシステムＢＳＳ及びＧＰＲＳシステムのパケット・スイッチング・コントローラＳＧＳＮが用いられるデータ転送システムで上述したが、本発明は、パケット・スイッチング・データ転送システムにおいて最も好ましい、ＴＤＭＡ及びＣＤＭＡデータ転送システムのような、他のデータ転送システムにも適用することができる。

【００５０】本発明は、上記実施例にのみ限定されず、それは、特許請求の範囲の範疇内で変更することができる。

【図面の簡単な説明】

【図１】ＧＰＲＳシステムのロジック構造を示す略ブロック図である。

【図２】ＧＰＲＳシステムの層構造及び層のデータ・フレーム構造を示す図である。

【図３】移動局及び移動局ネットワークにおける従来技術による暗号化キーの定義を示す略ブロック図である。

【図４】本発明の好ましい実施例による暗号化を示す図である。

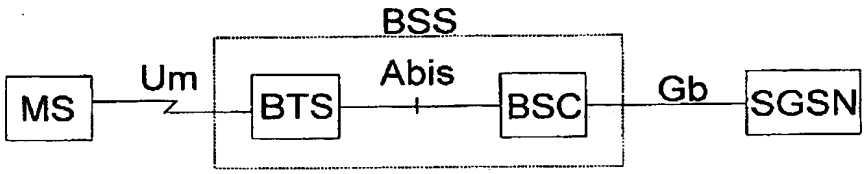
【図５】本発明の別の好ましい実施例による暗号化を示す図である。

【図６】実施例によるリンク層のデータ・フレーム構造を示す図である。

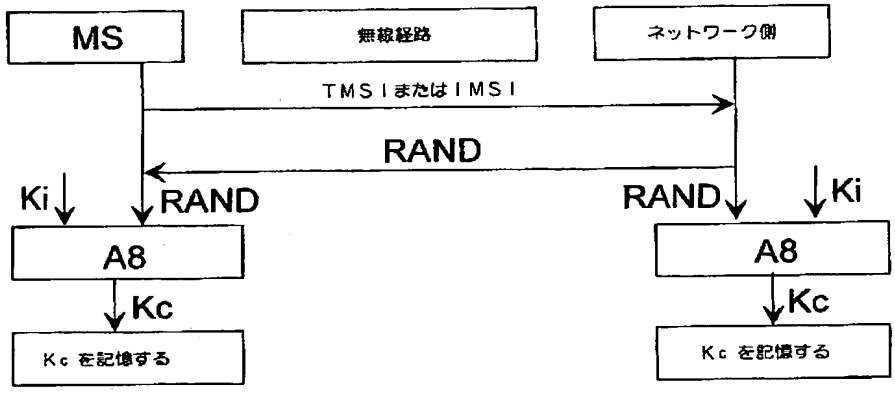
【図７】ポイント間接続を有する実施例による適応層のデータ・フレーム構造を示す図である。

＊【図８】多重ポイント接続を有する実施例による適応層のデータ・フレーム構造を示す図である。

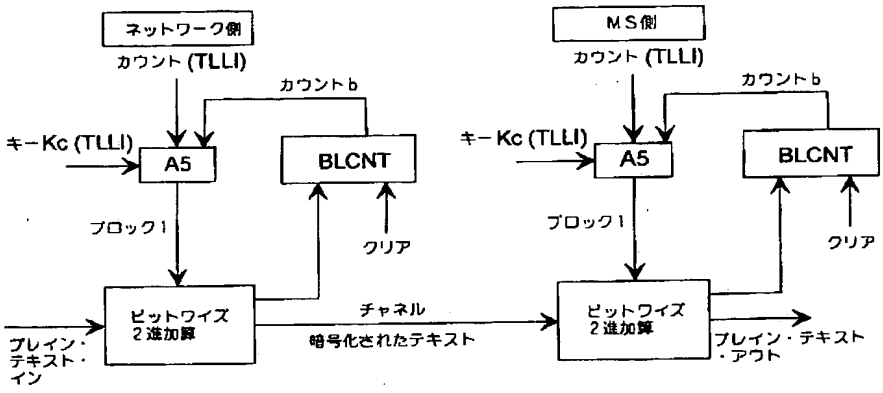
【図１】



【図３】



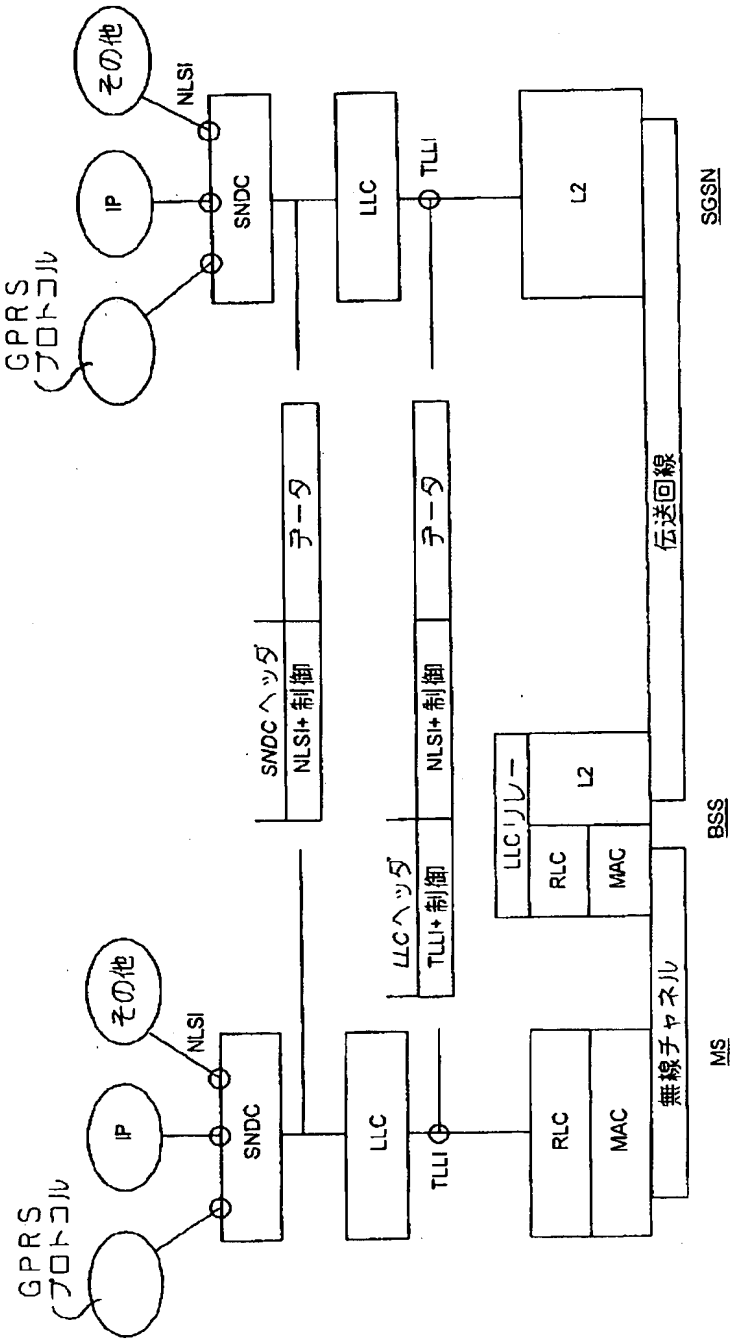
【図４】



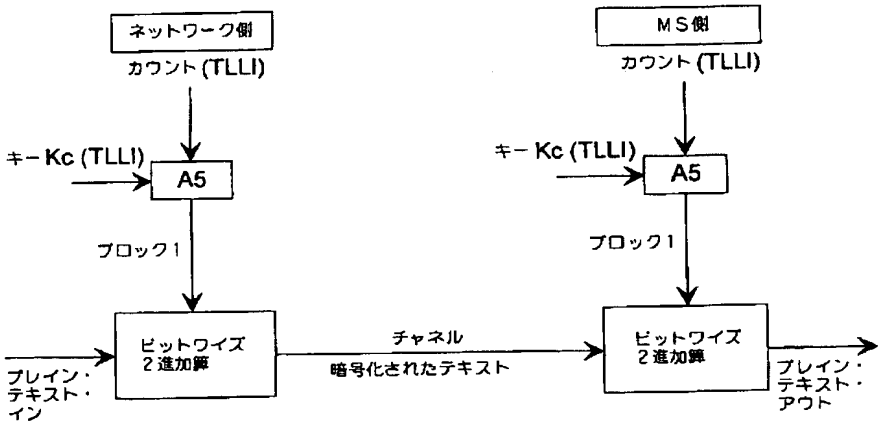
【図７】

ビット	8	7	6	5	4	3	2	1
オクト1	M	E	Pri		NLSI			
2	SDU番号（オプショナル）							
…	データ・セグメント							
N								

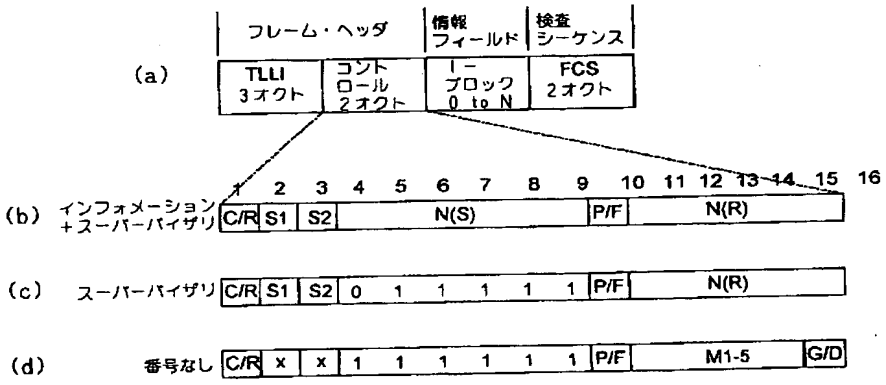
【図２】


GPRS
プロトコル
その他
IP
NLSI
SNDC
LLC
TLLI
L2
SGSN
伝送回線
SNDCヘッダ
NLSI+制御
データ
LLCヘッダ
TLLI+制御
データ
LLCリレー
L2
RLC
MAC
BSS
無線チャネル
MS
GPRS
プロトコル
その他
IP
NLSI
SNDC
LLC
TLLI
RLC
MAC

【図５】



【図６】



【図８】

ビット	8	7	6	5	4	3	2	1
オクト1	M	E	Pri		NLSI			
2	SDU番号							
…	データ・セグメント							
N								

フロントページの続き

(72)発明者　ヤリ　ヘーメーレイネン
フィンランド国，エフイーエン－33720
タンペレ，マティ　タピオンカトゥ　1
エフ　17

(72)発明者　ヤリ　ユオッペイ
フィンランド国，エフイーエン－00410
ヘルシンキ，ルートナンティンティエ　3
デー　30